



Direct Access

Es wird Zeit für eine neue Verbindung
Frank Carius

Erstklassige Lösungen,
innovative Produkte
und höchste Kompetenz.
Die perfekte Verbindung.
Für optimale Verbindungen.



Communication

Collaboration

Platform
Services

Managed
Service

Ihre E-Mail-Kommunikation
muss sicher funktionieren.

Mit den Gateway Solutions
von Net at Work wird sie sogar
komfortabler. Und effizienter.

NoSpamProxy Protection

- Anti-Spam
- Anti-Virus

NoSpamProxy Encryption

- Verschlüsselung
- SMIME / PGP /
PDFMail

NoSpamProxy Large Files

- Dateitransfer





Wir sind die Experten für die beste
IT-Lösung von allen:
Ihre maßgeschneiderte.

Standort Paderborn
Gründung 1995
40 Mitarbeiter

Microsoft Partner

- Gold Messaging
- Gold Communications
- Gold Collaboration and Content
- Gold Application Development

 **Net at Work**
Building IT-Excellence.

Direct Access

- VPN-Lösungen
 - Windows Routing und RAS
 - Verbindungsaufbau mühselig
 - PPTP ist unsicher
 - Firewall blockiert L2TP
 - 3rd Party VPN
 - Zusatzkosten
 - Zusätzliche Server
 - Getrenntes Management
 - Eigener Client muss verteilt werden
 - Browser-basiertes VPN
 - Gemischte Erfahrungen
- Betrieb (Windows VPN)
 - Benutzer „können“ kein VPN aufbauen
 - Manueller Verbindungsaufbau
 - Kein Management „von innen“

Brauchen wir noch ein VPN ?

- Mobile Geräte über ActiveSync
- Outlook über Outlook AnyWhere
- RDP über Terminal Server Gateway
- OneDrive for Business
- Webzugriff für
 - Outlook WebApp
 - CRM
 - SharePoint
 - SCOM, PRTG, ...
 - Exchange Control Panel
 - Lync Control Panel
 - Provisioning Systeme (z.B. Adaxes)

Aber ...

- Alles muss durch HTTPS
 - Andere Protokolle sind nicht „Firewall freundlich“
- Öffentliche Zertifikate
 - Da fremde Clients genutzt werden können
- Keine „integrierte“ Authentifizierung
 - Da kein Zugriff auf den KDC
- Outlook Anywhere/EWS
 - Kompletter Durchgriff auf fremden Geräten möglich
 - Keine „ActiveSync Policies“
 - Keine Quarantäne
- Nicht alle Dienste können „HTTPS“
- „Fremde“ Clients möglich
 - Keine Kontrolle
 - Keine Richtlinien
 - Keine Mindeststandards
 - Erschwerter Support

Direct Access Lösung

- Bestandteil von Windows Server
 - Windows 2008R2 Server, UAG für IPv4 Support, zwei Public IP
 - Windows 2012RTM/R2, Single IP, Kein UAG
- Clients
 - Windows 7 Enterprise
 - Windows 8 Enterprise
 - Windows 8.1 Enterprise
- Konfiguration per Gruppenrichtlinie
 - Einfachste Konfiguration für den Administrator
 - Server und Clients müssen Domainmitglied sein
 - GPO für Clients UND Server
- Always-On VPN
 - Anwender bauen keine Verbindung auf/ab
 - Management „von Innen“
 - PC muss nur an sein, keine Benutzeranmeldung erforderlich
 - Keine Unterscheidung zwischen Intern und Extern
- IPv6 als Basis, HTTPS als Transport

Direct Access – Wichtige Fakten

- Windows 2008R2/Windows 7 brauchen
 - IPv6 Deployment auf dem ersten Subnetz
 - DNS-Server mit IPv6-Adressen
 - Zwei aufeinanderfolgende öffentlicher IPv4-Adressen
 - PKI mit Zertifikaten und CRL
 - UAG für per IPv4 intern erreichbare Server
 - Gesonderter NLS-Server
- Windows 2012/Windows 8 machen es besser
 - NLS-Server kann auf DA-Server mitlaufen
 - Nur eine Public IPv4-Adresse
 - Keine PKI (außer mit Windows 7 Clients)
 - Kein IPv6 intern mehr erforderlich
 - Schnellerer Verbindungsaufbau
- Einschränkungen bleiben
 - IPv4-Only Hosts sind nur über „Namen“ erreichbar
 - Clientsoftware muss IPv6 unterstützen
 - Windows Enterprise Version als Desktop

Zusammenhänge

Routing

NAT

NAT64

DNS

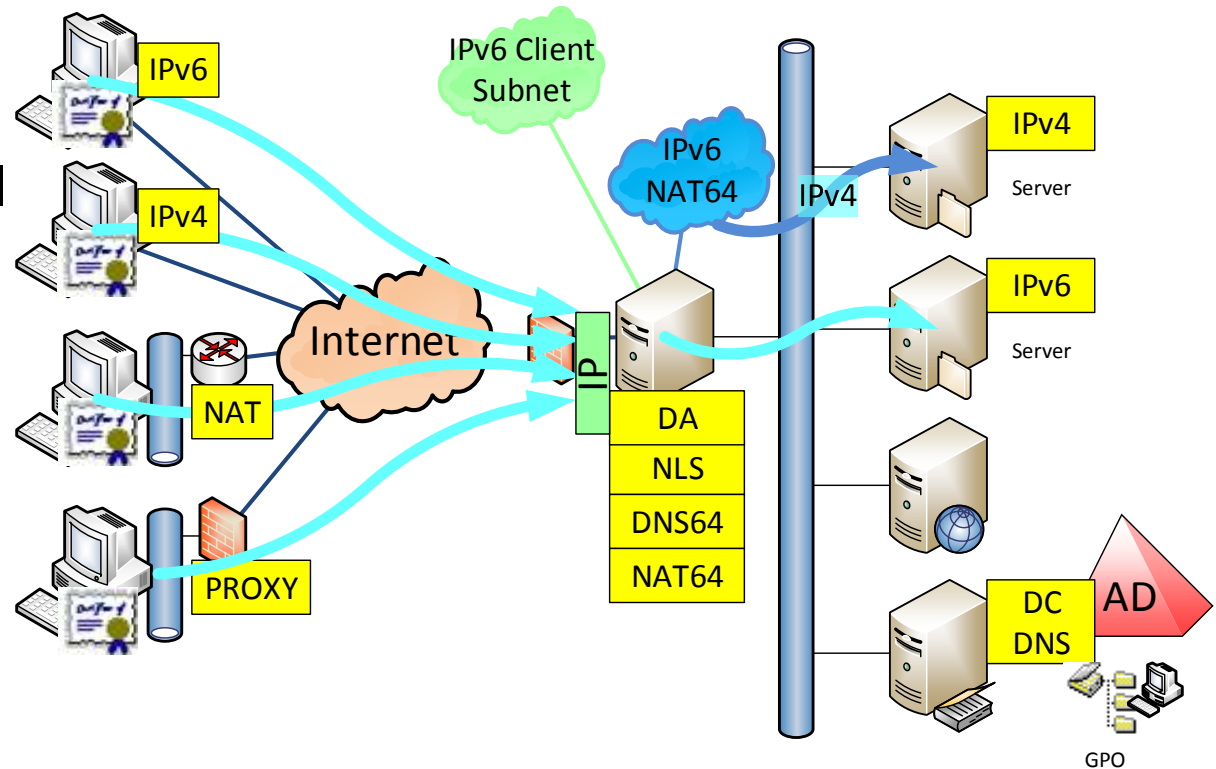
DNS64

IPHTTPS



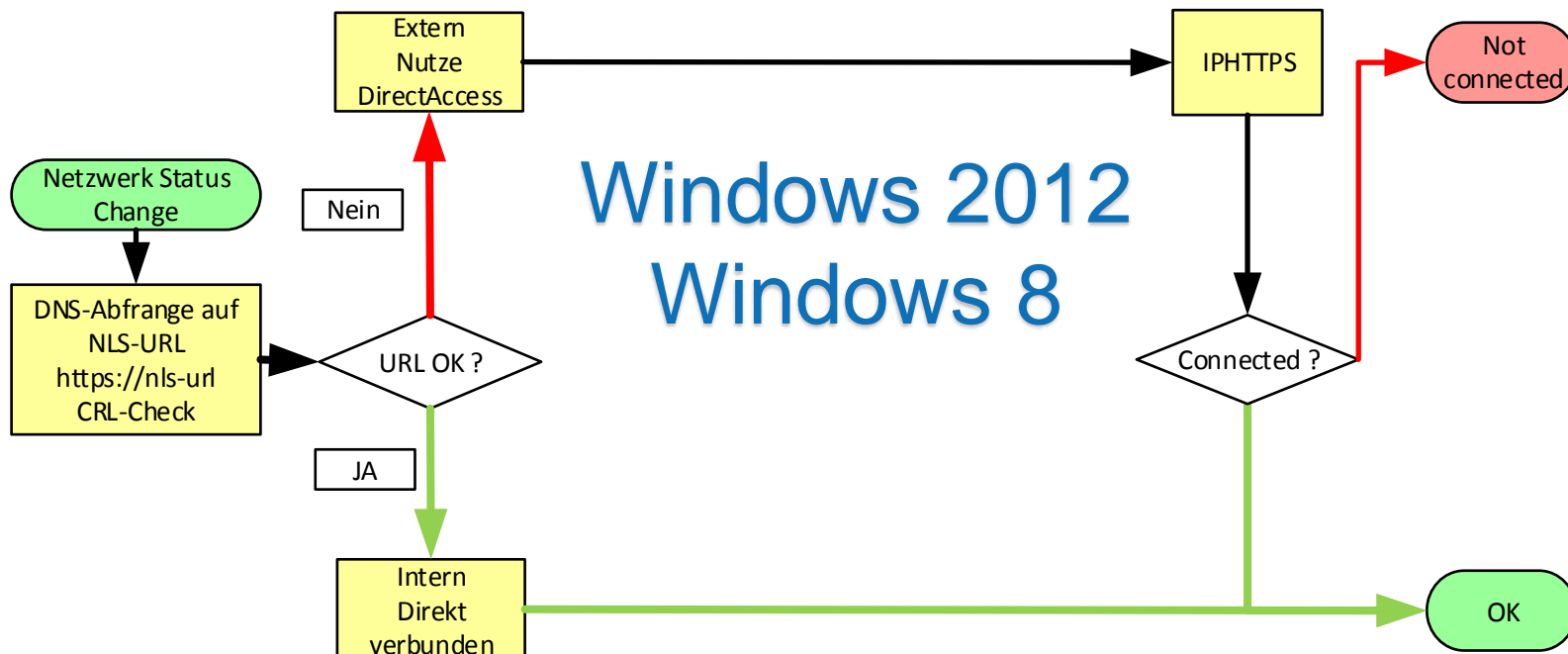
Basisnetzwerk

- Internes Netzwerk privaten IPv4
- Active Directory
- Gruppenrichtlinien
- DNS und DHCP
- Internet und Firewall



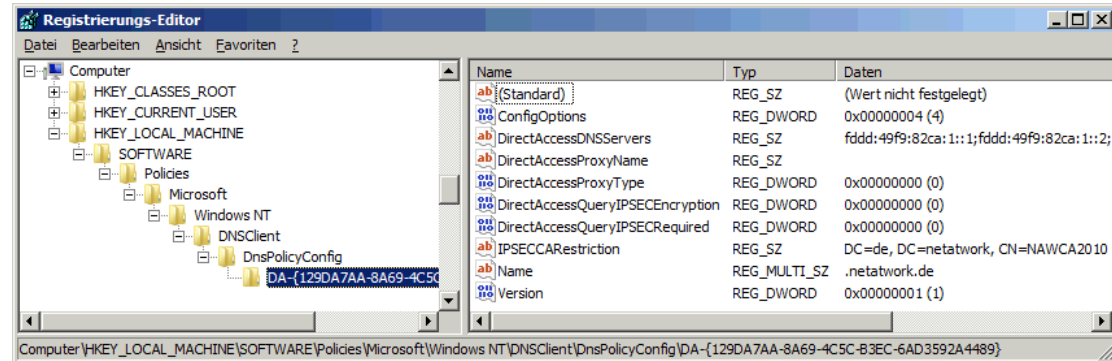
Network Location Service

- Woher weiß der Client, ob er Intern oder Extern ist ?
- Client prüft den Network Location Service
<https://nls.server.fqdn> – TLS Handshake muss passen
- **NLS ist „mission critical“ !**
- Client baut Verbindung auf

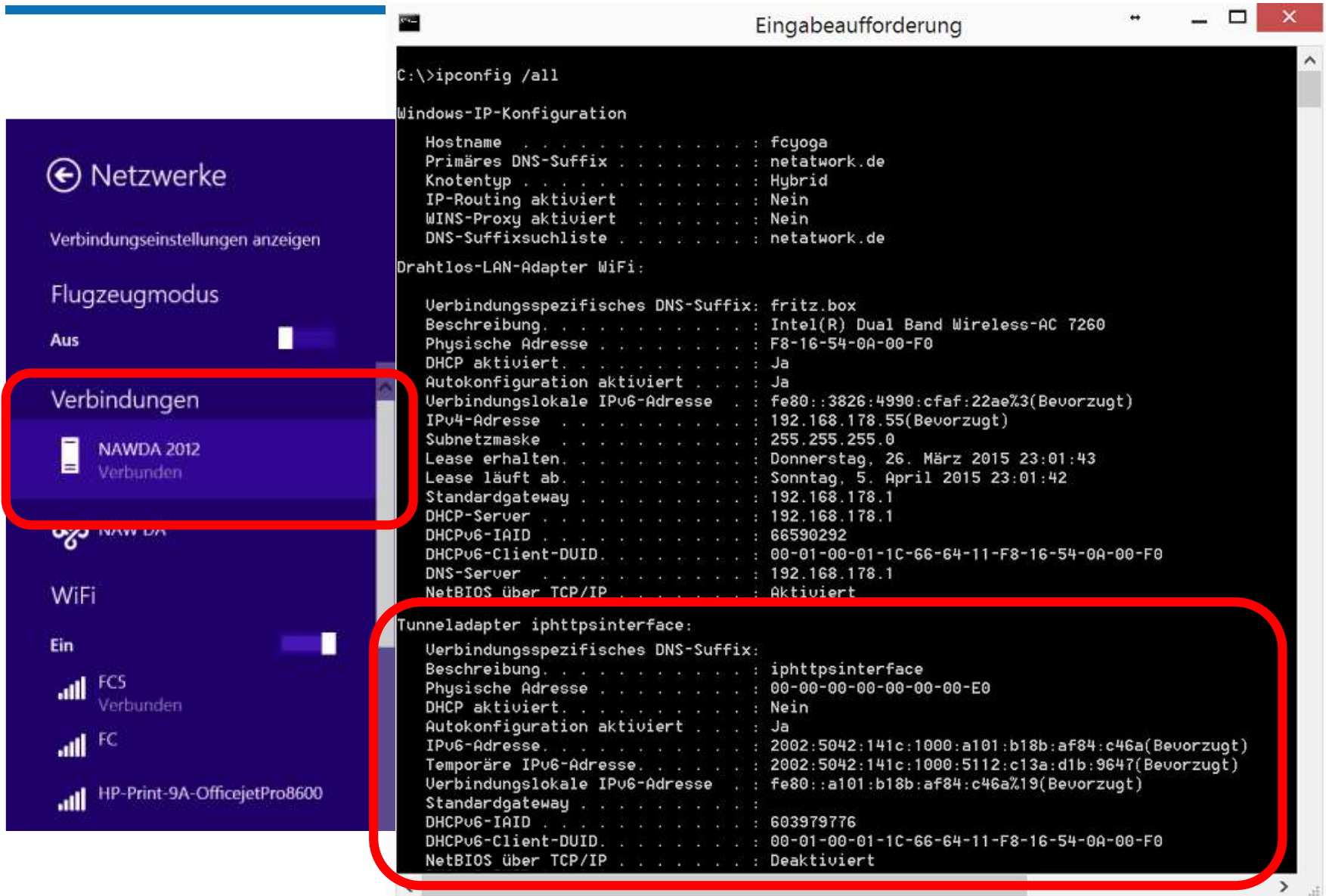


Wie wird der Client konfiguriert ?

- DA Assistent legt „Gruppenrichtlinien“ an
 - Enthalten den NLS-Server
 - Enthalten den DA-Server
 - Enthalten Zertifikatinformationen
 - Enthalten DNS-Informationen (Name Resolution Policy Table, NRPT)
- Client stellt Verbindung her
 - Prüft NLS-Service
 - Baut IPHTTP-Tunnel auf
 - Bekommt IPv6-Adresse aus dem Pool des Direct Access-Servers



IPConfig auf einem DA-Client



The image shows a Windows 8.1 desktop environment. On the left, the 'Netzwerke' (Network) control panel is open, with the 'Verbindungen' (Connections) section highlighted in a red box. It shows a mobile device 'NAWDA 2012' connected via 'Verbindungen' and a 'WiFi' section with 'FCS' and 'FC' networks connected. On the right, a command prompt window titled 'Eingabeaufforderung' displays the output of the 'ipconfig /all' command. The output is divided into sections: 'Windows-IP-Konfiguration', 'Drahtlos-LAN-Adapter WiFi:', and 'Tunneladapter iphttpsinterface:'. The 'Tunneladapter iphttpsinterface:' section is highlighted in a red box. The command prompt shows the following configuration details:

```
C:\>ipconfig /all

Windows-IP-Konfiguration

    Hostname . . . . . : fcyoga
    Primäres DNS-Suffix . . . . . : netatwork.de
    Knotentyp . . . . . : Hybrid
    IP-Routing aktiviert . . . . . : Nein
    WINS-Proxy aktiviert . . . . . : Nein
    DNS-Suffixsuchliste . . . . . : netatwork.de

Drahtlos-LAN-Adapter WiFi:

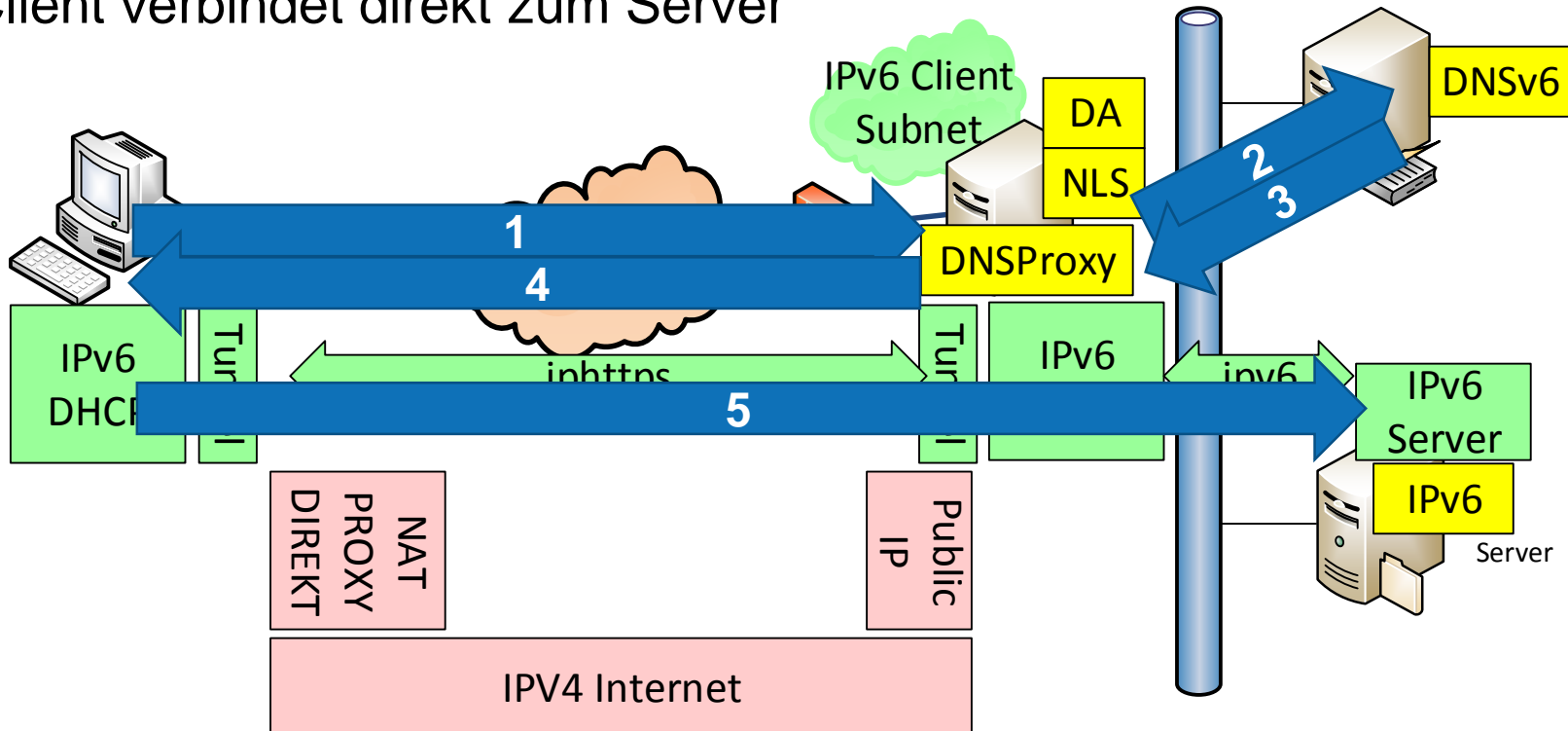
    Verbindungsspezifisches DNS-Suffix: fritz.box
    Beschreibung. . . . . : Intel(R) Dual Band Wireless-AC 7260
    Physische Adresse . . . . . : F8-16-54-0A-00-F0
    DHCP aktiviert. . . . . : Ja
    Autokonfiguration aktiviert . . . : Ja
    Verbindungslokale IPv6-Adresse . . : fe80::3826:4990:cfaf:22ae%3(Bevorzugt)
    IPv4-Adresse . . . . . : 192.168.178.55(Bevorzugt)
    Subnetzmaske . . . . . : 255.255.255.0
    Lease erhalten. . . . . : Donnerstag, 26. März 2015 23:01:43
    Lease läuft ab. . . . . : Sonntag, 5. April 2015 23:01:42
    Standardgateway . . . . . : 192.168.178.1
    DHCP-Server . . . . . : 192.168.178.1
    DHCPv6-IAID . . . . . : 66590292
    DHCPv6-Client-DUID. . . . . : 00-01-00-01-1C-66-64-11-F8-16-54-0A-00-F0
    DNS-Server . . . . . : 192.168.178.1
    NetBIOS über TCP/IP . . . . . : Aktiviert

Tunneladapter iphttpsinterface:

    Verbindungsspezifisches DNS-Suffix:
    Beschreibung. . . . . : iphttpsinterface
    Physische Adresse . . . . . : 00-00-00-00-00-00-E0
    DHCP aktiviert. . . . . : Nein
    Autokonfiguration aktiviert . . . : Ja
    IPv6-Adresse. . . . . : 2002:5042:141c:1000:a101:b18b:af84:c46a(Bevorzugt)
    Temporäre IPv6-Adresse. . . . . : 2002:5042:141c:1000:c13a:d1b:9647(Bevorzugt)
    Verbindungslokale IPv6-Adresse . . : fe80::a101:b18b:af84:c46a%19(Bevorzugt)
    Standardgateway . . . . . :
    DHCPv6-IAID . . . . . : 603979776
    DHCPv6-Client-DUID. . . . . : 00-01-00-01-1C-66-64-11-F8-16-54-0A-00-F0
    NetBIOS über TCP/IP . . . . . : Deaktiviert
```

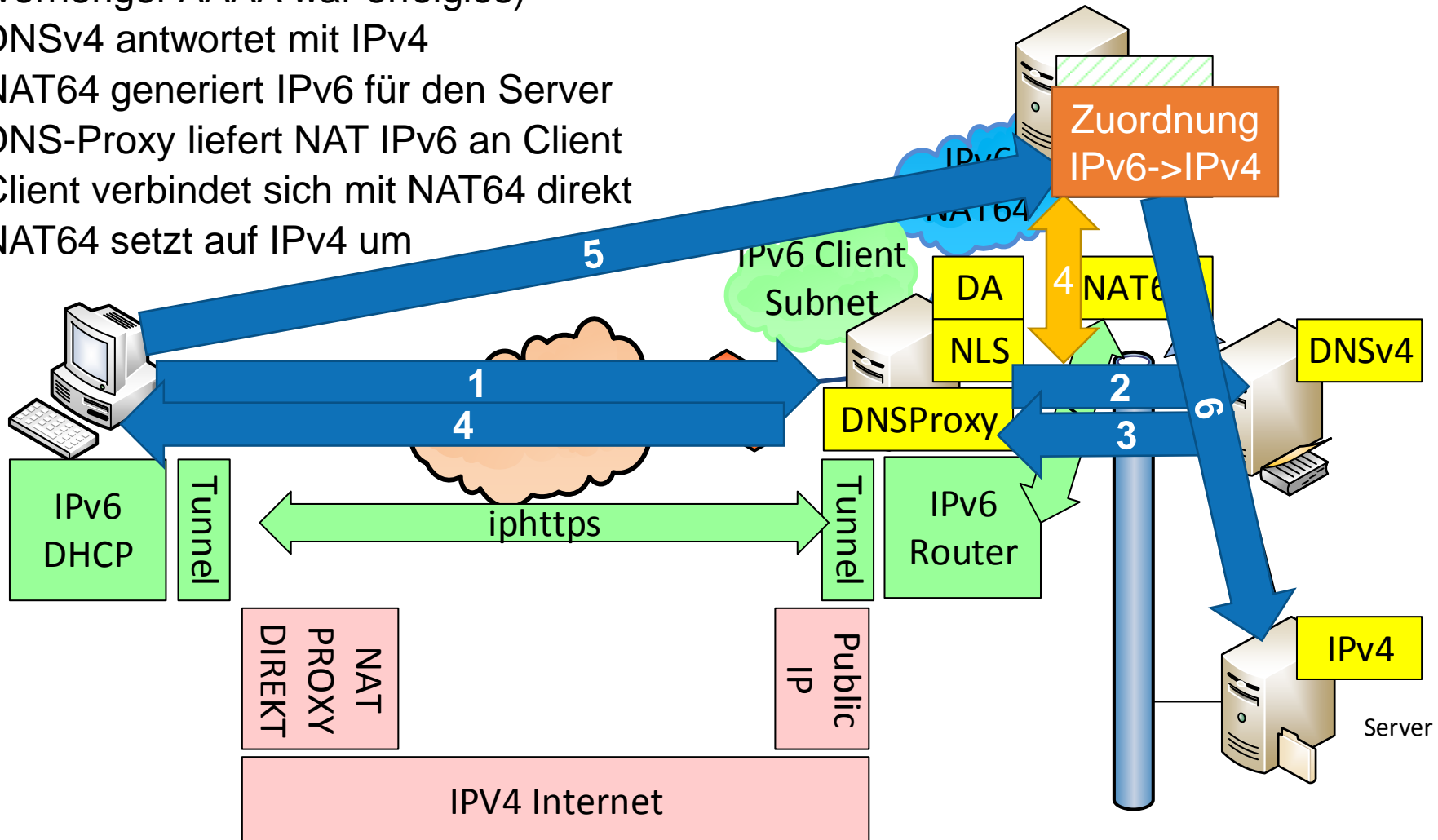
DNS und IP-Routing: IPv6 Server

- Client fragt den DNS-Proxy nach dem Namen
- DNS-Proxy stellt AAAA-Query an DNS
- DNSv6 antwortet mit IPv6
- DNSProxy liefert IPv6 an Client
- Client verbindet direkt zum Server



DNS und IP-Routing: IPv4 Server

- Client fragt den DNS-Proxy nach dem Namen
- DNS-Proxy stellt A-Query an DNS (vorheriger AAAA war erfolglos)
- DNSv4 antwortet mit IPv4
- NAT64 generiert IPv6 für den Server
- DNS-Proxy liefert NAT IPv6 an Client
- Client verbindet sich mit NAT64 direkt
- NAT64 setzt auf IPv4 um

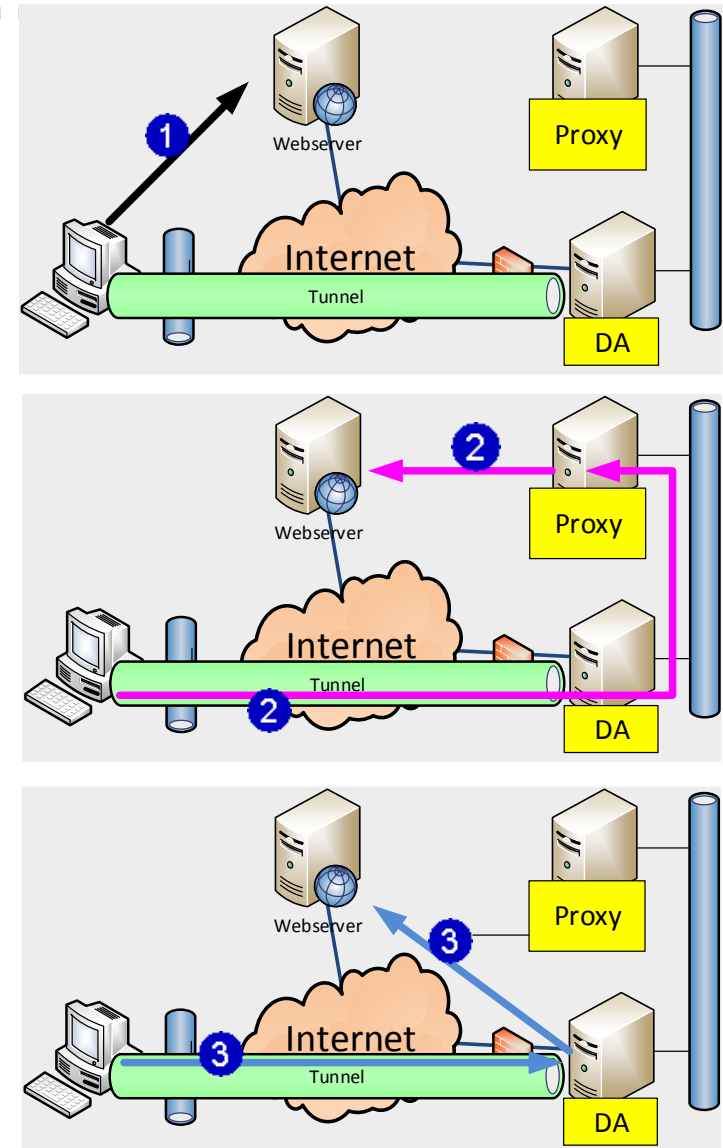


DNS64 und NAT64

- Ein DA-Client kann NUR mit IPv6-Gegenstellen sprechen
- Ein DA-Client fragt immer den DNS-Proxy auf dem DA-Server
- Der DNS-Proxy fragt den internen DNS-Server
- DNS-Server liefert IPv6 oder IPv4-Adresse
 - IPv6-Antwort nur, wenn per IPv6 erreichbar
- IPv6-Server werden direkt angesprochen
 - intern ist IPv6 korrekt konfiguriert
 - Bitte kein ISATAP !!!
- IPv4-Server werden hinter einer IPv6 Adresse per Reverse-NAT versteckt
 - NAT64-Komponente setzt Pakete entsprechend um
- DA-Client kann nie IPv4-Adressen direkt ansprechen
 - Hosts müssen per DNS aufgelöst werden, um NAT64 zu aktivieren
- NAT64 ist erst seit Windows 2012 „eingebaut“
 - Mit Windows 2008R2 DA musste ein NAT64/DNS64 Service extra installiert werden, z.B. UAG

Internet Zugriff für DA Clients

- Bypass
 - Internet Traffic direkt zum Ziel
 - Kein Verkehr auf dem Tunnel
 - Auch für selektive Hosts und Domains
- Tunnel Mode mit HTTP-Proxy
 - Browser via HTTP-Proxy
 - Zentrale Steuerung/Filterung
 - Doppelter Verkehr am Firmen-Link
- Tunnel ohne Proxy
 - Source IP des Direct Access wird genutzt
 - Direct Access muss also „raus“ dürfen
- Lokaler Traffic
 - Zugriffe auf Dienste im lokalen Netz gehen immer, z.B. Drucker



- Management von Clients
 - Über Direct Access können Clients vom zentralen LAN verwaltet werden
 - Voraussetzung ist IPv6 !!!
 - Direct Access kann sogar für „Management Only“ eingesetzt werden
- Hochverfügbarkeit
 - DirectAccess ist HTTPS
 - Lastverteilung mit NLB oder externem Loadbalancer
 - Denken Sie an NLS Verfügbarkeit !!
- Geografische Steuerung
 - Mehrere DA-Server in verschiedenen Ländern möglich
 - Client nutzt immer den gleichen DA-Zugang
 - Steuerung per Gruppenrichtlinien und Computergruppen

Einrichtung und Konfiguration

Rollen

Features

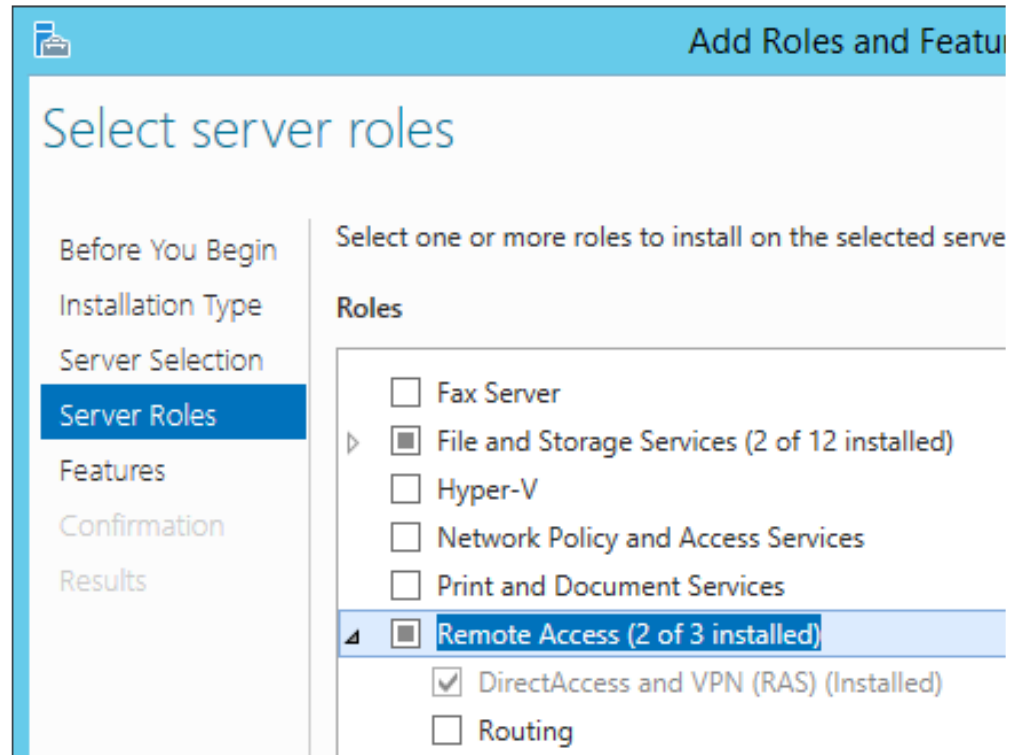
Adressen

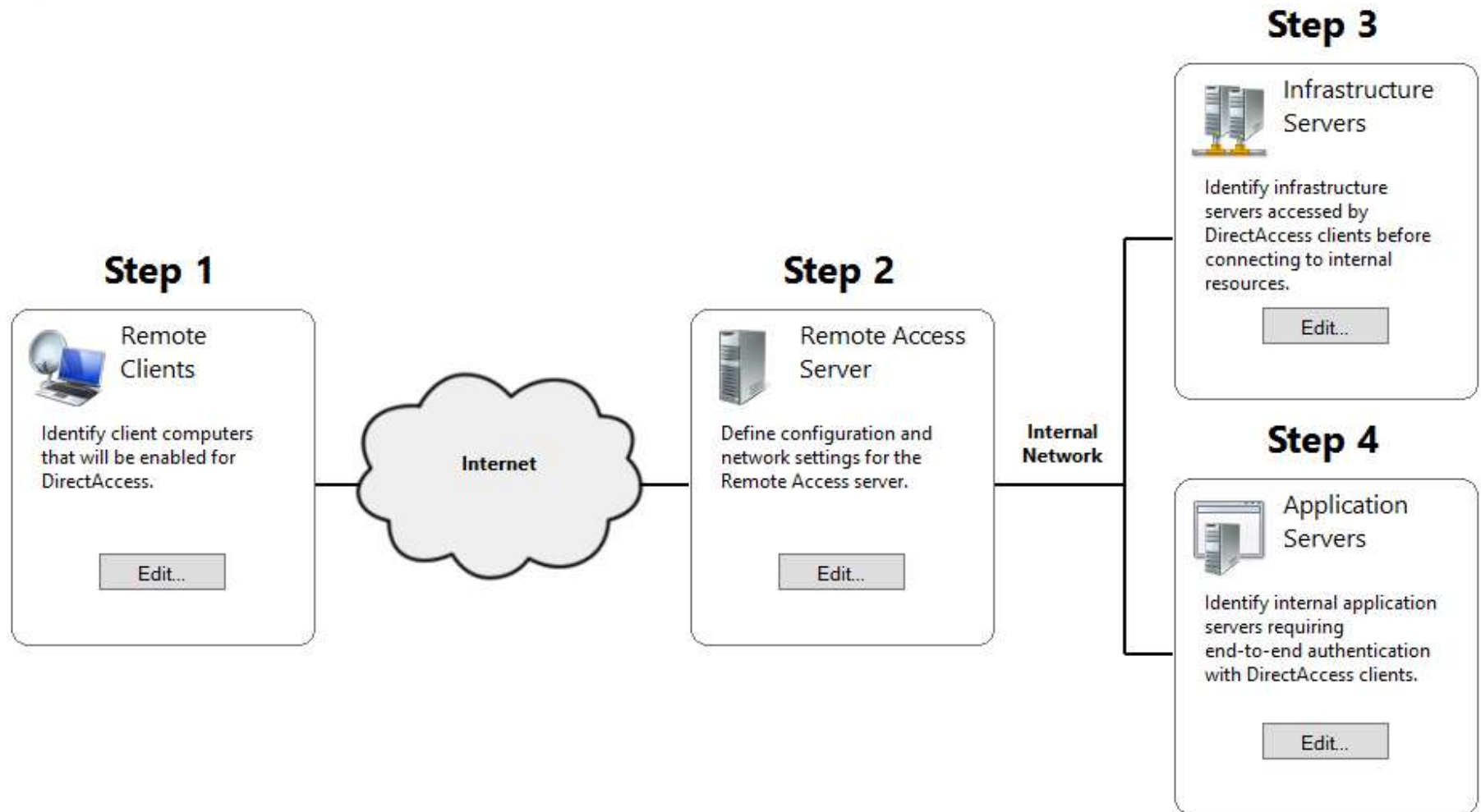
Richtlinien



Schritte der Einrichtung

- Basis schaffen
 - Windows 2012 R2 Server
 - 1x Netzwerk nach „draußen“
 - 1x Firewall 443 eingehend
 - 1x DNS-Eintrag extern
 - 1x DNS-Eintrag intern (Connectivity Check)
 - 1x Netzwerk nach „drinnen“
 - Mitglied der Domäne
- Add Roles & Features
 - Remote Access
 - Updates installieren
- Konfigurieren
- Testen
- Ausrollen



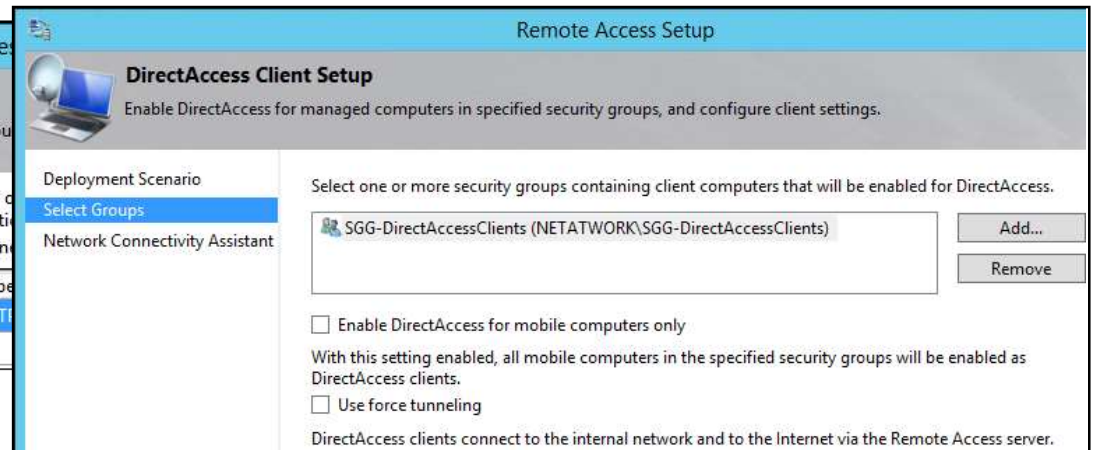
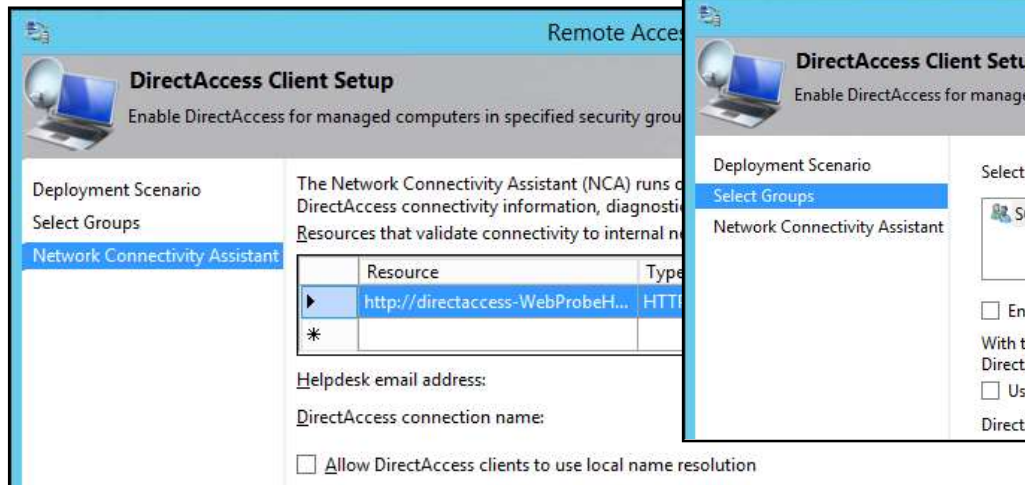
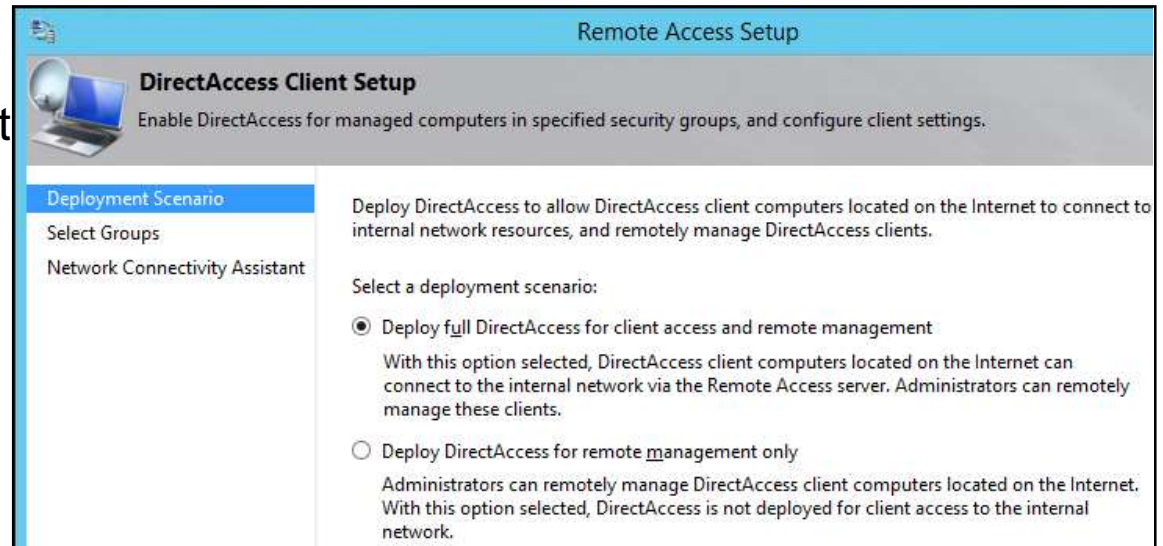


Schritt 1: Remote Client festlegen

- Deployment Szenario
 - Client und Management
 - Management only

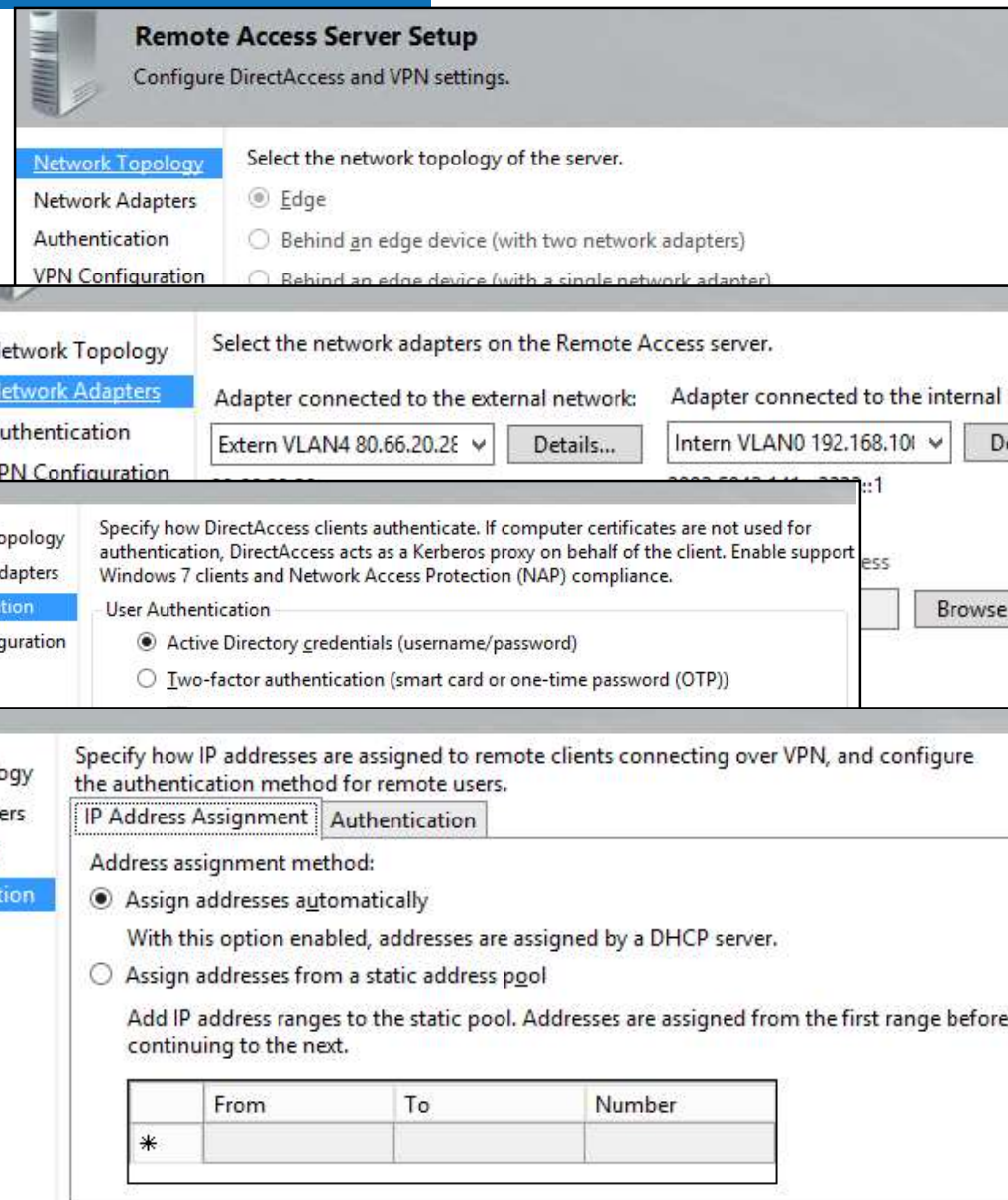
- Zielclients
 - Windows Gruppen

- Connectivity Check
 - Mit „VPN Name“



Schritt 2: Konfiguration des DA-Server

- Topologie
 - Ohne Firewall d.h. ein Bein im Internet, eines intern
 - Hinter einer Firewall (zwei Netzwerkkarten)
 - Hinter einer Firewall (eine Netzwerkkarte)
- Konfiguration der Netzwerkkarten
 - IP-Adressen
 - Zertifikat
- Authentifizierung
 - AD oder MultiFaktor
 - Optional Zertifikate (erforderlich mit Windows Clients)
 - Optional NAP
- VPN Konfiguration



Remote Access Server Setup
Configure DirectAccess and VPN settings.

Network Topology Select the network topology of the server.

Network Adapters Edge

Authentication Behind an edge device (with two network adapters)

VPN Configuration Behind an edge device (with a single network adapter)

Network Adapters Select the network adapters on the Remote Access server.

Adapter connected to the external network: Extern VLAN4 80.66.20.28 Details... Adapter connected to the internal network: Intern VLAN0 192.168.10.1

Authentication Specify how DirectAccess clients authenticate. If computer certificates are not used for authentication, DirectAccess acts as a Kerberos proxy on behalf of the client. Enable support for Windows 7 clients and Network Access Protection (NAP) compliance.

User Authentication

Active Directory credentials (username/password)

Two-factor authentication (smart card or one-time password (OTP))

VPN Configuration Specify how IP addresses are assigned to remote clients connecting over VPN, and configure the authentication method for remote users.

IP Address Assignment Authentication

Address assignment method:

Assign addresses automatically

With this option enabled, addresses are assigned by a DHCP server.

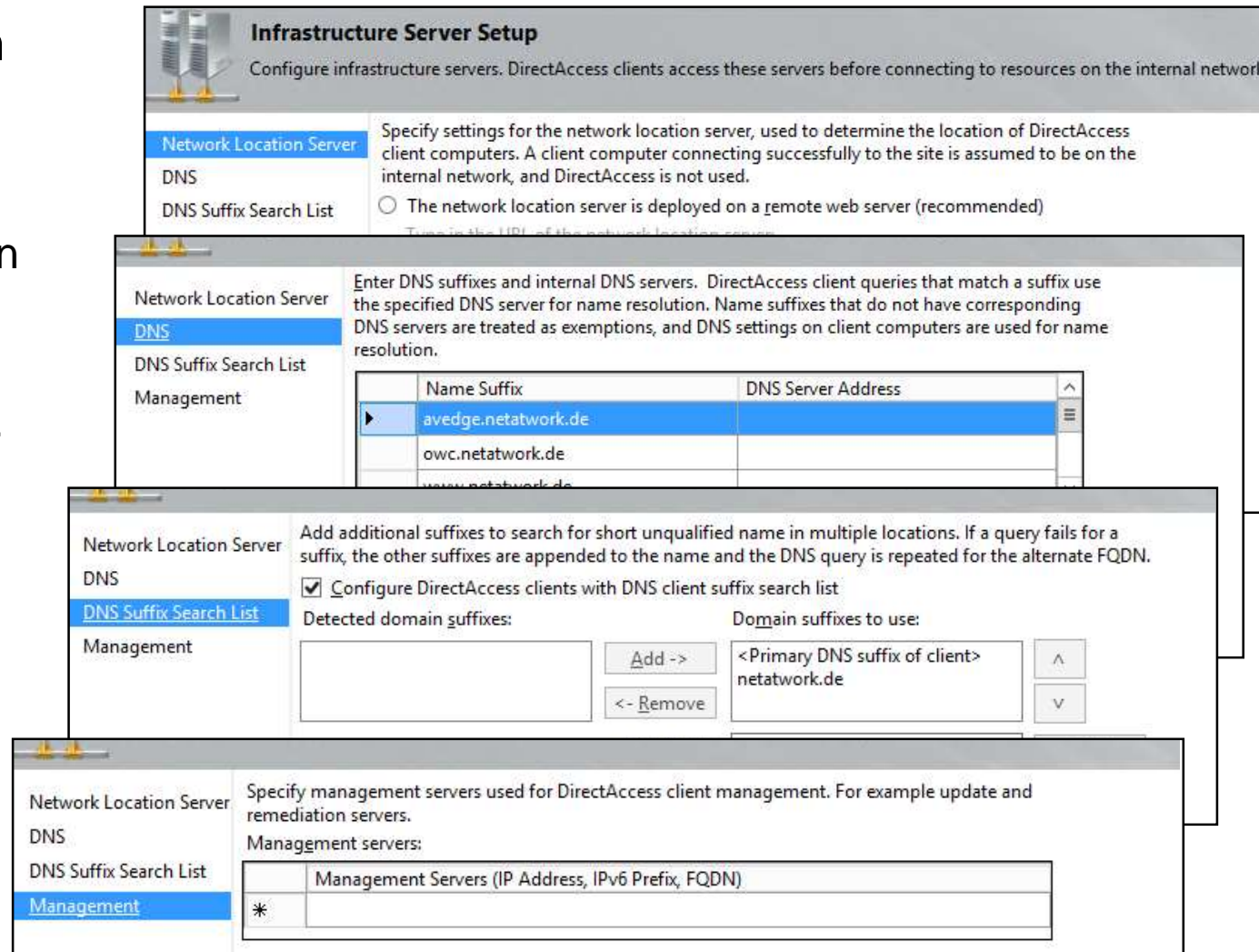
Assign addresses from a static address pool

Add IP address ranges to the static pool. Addresses are assigned from the first range before continuing to the next.

	From	To	Number
*			

Step 3: Infrastruktur Server

- Network Location Server
 - Wie der Client erkennt, dass er extern oder intern ist
- DNS
 - Alternative DNS-Server und Ausnahmen pflegen
- DNS Suffix
 - Suchreihenfolge
- Management Servers
 - SCOM u.a.



Infrastructure Server Setup
Configure infrastructure servers. DirectAccess clients access these servers before connecting to resources on the internal network.

Network Location Server
Specify settings for the network location server, used to determine the location of DirectAccess client computers. A client computer connecting successfully to the site is assumed to be on the internal network, and DirectAccess is not used.
 The network location server is deployed on a remote web server (recommended)

DNS
Enter DNS suffixes and internal DNS servers. DirectAccess client queries that match a suffix use the specified DNS server for name resolution. Name suffixes that do not have corresponding DNS servers are treated as exemptions, and DNS settings on client computers are used for name resolution.

Name Suffix	DNS Server Address
avedge.netatwork.de	
owc.netatwork.de	
www.netatwork.de	

DNS Suffix Search List
Add additional suffixes to search for short unqualified name in multiple locations. If a query fails for a suffix, the other suffixes are appended to the name and the DNS query is repeated for the alternate FQDN.
 Configure DirectAccess clients with DNS client suffix search list

Detected domain suffixes: [] [Add ->] [Remove -<]
Domain suffixes to use: <Primary DNS suffix of client> netatwork.de [^] [v]

Management
Specify management servers used for DirectAccess client management. For example update and remediation servers.
Management servers:

Management Servers (IP Address, IPv6 Prefix, FQDN)
*

Typische „Ausnahmen“

- CRL Verteilpunkte
- IPHTTP-Server
- VPN-Server
- Lync Edge Server
- Extern per HTTP erreichbare Systeme
 - Exchange OWA
 - SharePoint
 - RDP-Gateway
 - UAG Portal
 - Office 365 Dienste
 - ADFS-Server

Step 4: Internal Application Server



DirectAccess Application Server Setup

Optionally configure authentication between DirectAccess clients and internal application servers.

By default, DirectAccess requires IPsec authentication and encryption between the DirectAccess client and server. In addition, you can optionally require end-to-end authentication and encryption between DirectAccess clients and selected internal application servers.

- Do not extend authentication to application servers
- Extend authentication to selected application servers

Select the security groups containing the servers:

Add...

Remove

- Allow access only to servers included in the security groups

With this option enabled, clients can only access application servers in the specified security groups. Clients can still access infrastructure servers, including domain controllers, DNS servers, and servers used for DirectAccess client management.

- Do not encrypt traffic. Use authentication only

With this setting enabled, end-to-end traffic is authenticated but not encrypted. This option is less secure. Authentication without encryption is supported only for application servers running Windows Server 2008 R2 or a later operating system.

Betrieb

Client, Server, Dienste, Counter



Management Client Dashboard

Remote Access Dashboard

Server Status

Operations Status

- NAWDA.netatwork.de
 - DirectAccess
 - 6to4
 - DNS
 - DNS64
 - Domain controller
 - IP-HTTPS
 - IPsec
 - Kerberos
 - NAT64
 - Network adapters
 - Network location server
 - Network security
 - Services

[Operations Status page](#)

Configuration Status

12/3/2014 4:13:31 PM

The configuration was distributed successfully

DirectAccess and VPN Client Status

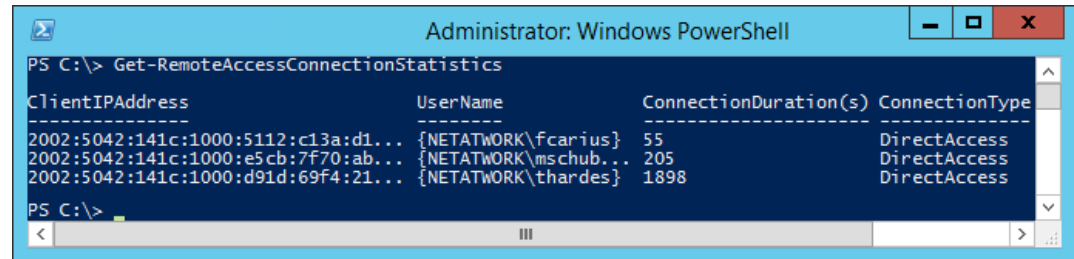
Total active clients:	1	Total transferred data:	9.12 GB in/57.83 GB out
Total active DirectAccess clients	1	Maximum client connections:	14
Total active VPN clients:	0	Total active unique users:	0
Total cumulative connections:	4709		

[Remote Client Status page](#)

PowerShell auf dem Server

- **Get-RemoteAccessConnectionStatistics**

Anzeige der aktuell verbundenen Clients



```
Administrator: Windows PowerShell
PS C:\> Get-RemoteAccessConnectionStatistics

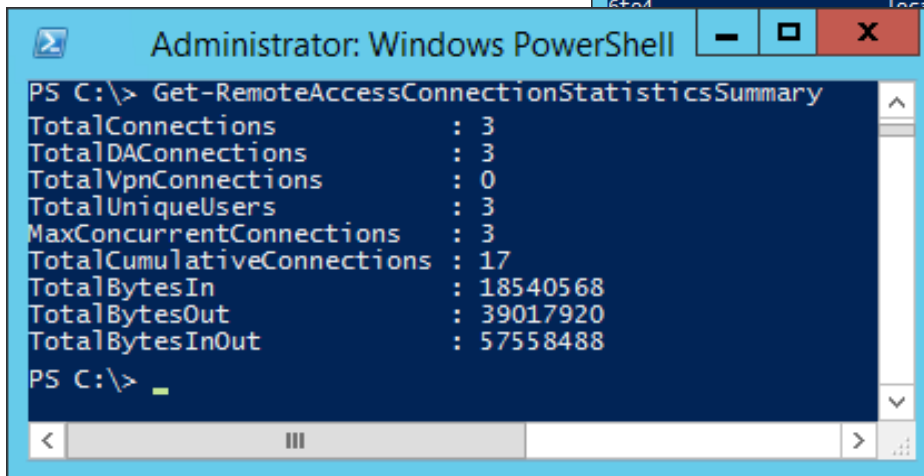
ClientIPAddress      UserName              ConnectionDuration(s) ConnectionType
-----
2002:5042:141c:1000:5112:c13a:d1... {NETATWORK\fcarius} 55               DirectAccess
2002:5042:141c:1000:e5cb:7f70:ab... {NETATWORK\mschub... 205              DirectAccess
2002:5042:141c:1000:d91d:69f4:21... {NETATWORK\thardes} 1898             DirectAccess

PS C:\>
```

- **Get-RemoteAccessHealth**

- **Get-RemoteAccessConnectionStatisticsSummary**

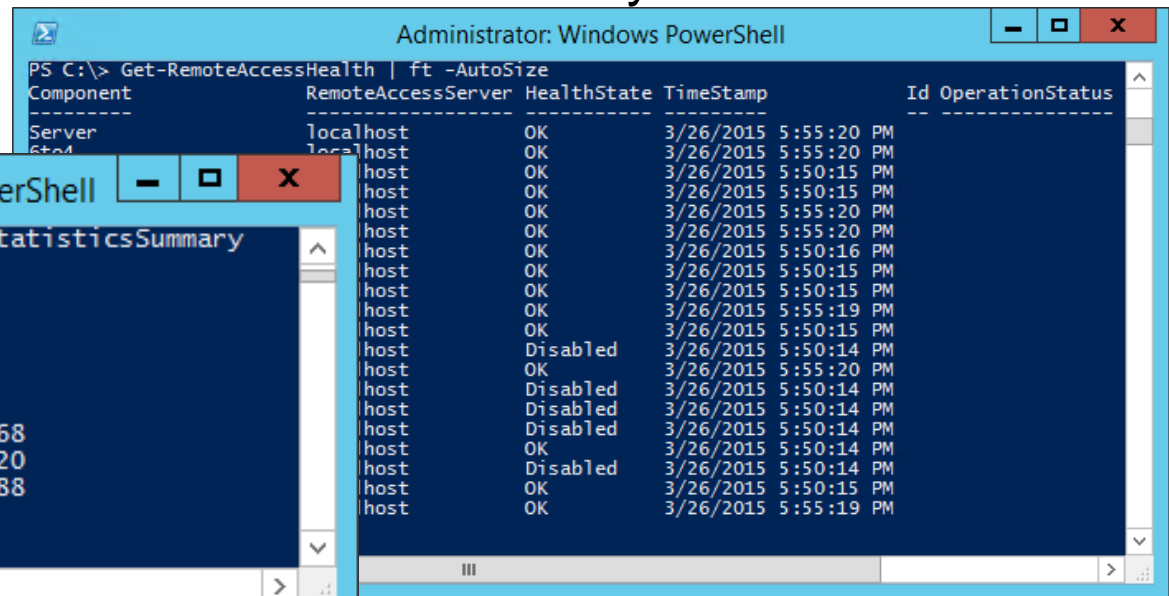
Anzeige der Summen



```
Administrator: Windows PowerShell
PS C:\> Get-RemoteAccessConnectionStatisticsSummary

TotalConnections      : 3
TotalDAConnections    : 3
TotalVpnConnections   : 0
TotalUniqueUsers      : 3
MaxConcurrentConnections : 3
TotalCumulativeConnections : 17
TotalBytesIn          : 18540568
TotalBytesOut         : 39017920
TotalBytesInOut       : 57558488

PS C:\>
```



```
Administrator: Windows PowerShell
PS C:\> Get-RemoteAccessHealth | ft -AutoSize

Component      RemoteAccessServer HealthState TimeStamp      Id OperationStatus
-----
Server         localhost        OK          3/26/2015 5:55:20 PM
6764          localhost        OK          3/26/2015 5:55:20 PM
host           host             OK          3/26/2015 5:50:15 PM
host           host             OK          3/26/2015 5:50:15 PM
host           host             OK          3/26/2015 5:55:20 PM
host           host             OK          3/26/2015 5:50:15 PM
host           host             OK          3/26/2015 5:55:20 PM
host           host             OK          3/26/2015 5:50:16 PM
host           host             OK          3/26/2015 5:50:15 PM
host           host             OK          3/26/2015 5:50:15 PM
host           host             OK          3/26/2015 5:55:19 PM
host           host             OK          3/26/2015 5:50:15 PM
host           host             Disabled   3/26/2015 5:50:14 PM
host           host             OK          3/26/2015 5:55:20 PM
host           host             Disabled   3/26/2015 5:50:14 PM
host           host             Disabled   3/26/2015 5:50:14 PM
host           host             Disabled   3/26/2015 5:50:14 PM
host           host             OK          3/26/2015 5:50:14 PM
host           host             Disabled   3/26/2015 5:50:14 PM
host           host             OK          3/26/2015 5:50:15 PM
host           host             OK          3/26/2015 5:55:19 PM
```

Fehlersuche auf dem Client

- netsh namespace show policy
- netsh inter httpstunnel show statistic
- netsh inter httpstunnel show interface

```
PS C:\Users\adm-fcarius> netsh int httpstunnel show stat




Interface IPHTTPSInterface Parameters
-----
Total bytes received      : 1260537242
Total bytes sent          : 2903803810

Most Recent Client Address      Total Bytes In  Total Bytes Out
-----
PS C:\Users\adm-fcarius> netsh int httpstunnel show int

Interface IPHTTPSInterface Parameters
-----
Role           : server
URL            : https://da.netatwork.de:443/IPHTTPS
Client authentication mode : none
Last Error Code : 0x0
Interface Status : IPHTTPS interface active
```

Windows-Firewall mit erweitert

- Eingehende Regeln
- Ausgehende Regeln
- Verbindungssicherheitsregeln
- Überwachung

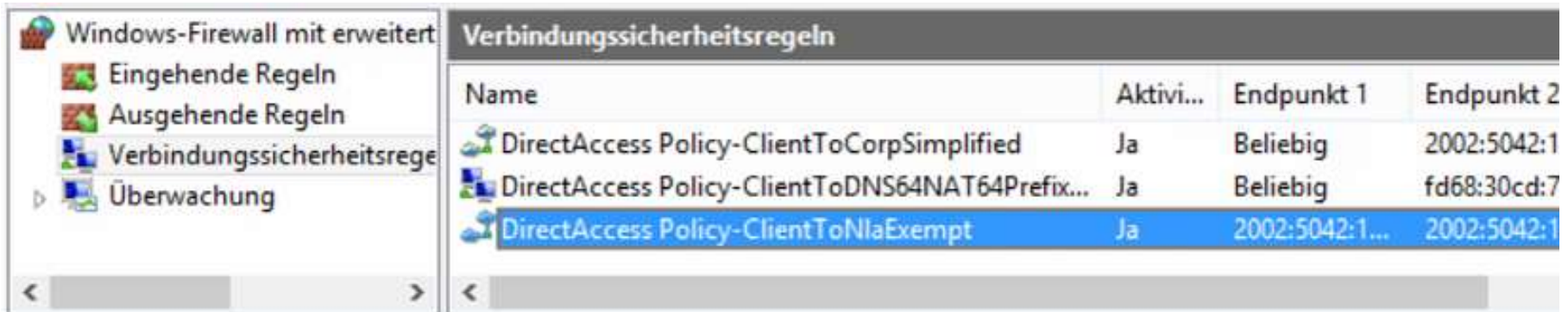
Verbindungssicherheitsregeln						
Name	Aktivi...	Endpunkt 1	Endpunkt 2	Authentifizierungsmodus	Authentifizierur	
 DirectAccess Policy-ClientToCorpSimplified	Ja	Beliebig	2002:5042:1...	Eingehend und ausgeh...	Benutzerdefinie	
 DirectAccess Policy-ClientToDNS64NAT64Prefix...	Ja	Beliebig	fd68:30cd:7...	Nicht authentifizieren	Keine Authentif	
 DirectAccess Policy-ClientToNlaExempt	Ja	2002:5042:1...	2002:5042:1...	Nicht authentifizieren	Keine Authentif	

Fehlersuche auf dem Client

- IPConfig /ALL

```
Tunneladapter iphttpsinterface:  
  Verbindungsspezifisches DNS-Suffix:  
  Beschreibung . . . . . : iphttpsinterface  
  Physische Adresse . . . . . : 00-00-00-00-00-00-00-E0  
  DHCP aktiviert. . . . . : Nein  
  Autokonfiguration aktiviert . . . . . : Ja  
  IPv6-Adresse . . . . . : 2002:5042:141c:1000:a101:b18b:af84:c46a(Bevorzugt)  
  Temporäre IPv6-Adresse . . . . . : 2002:5042:141c:1000:5112:c13a:d1b:9647(Bevorzugt)  
  Verbindungslokale IPv6-Adresse . . . . . : fe80::a101:b18b:af84:c46a%19(Bevorzugt)  
  Standardgateway . . . . . :  
  DHCPv6-IAID . . . . . : 603979776  
  DHCPv6-Client-DUID . . . . . : 00-01-00-01-1C-66-64-11-F8-16-54-0A-00-F0  
  NetBIOS über TCP/IP . . . . . : Deaktiviert
```

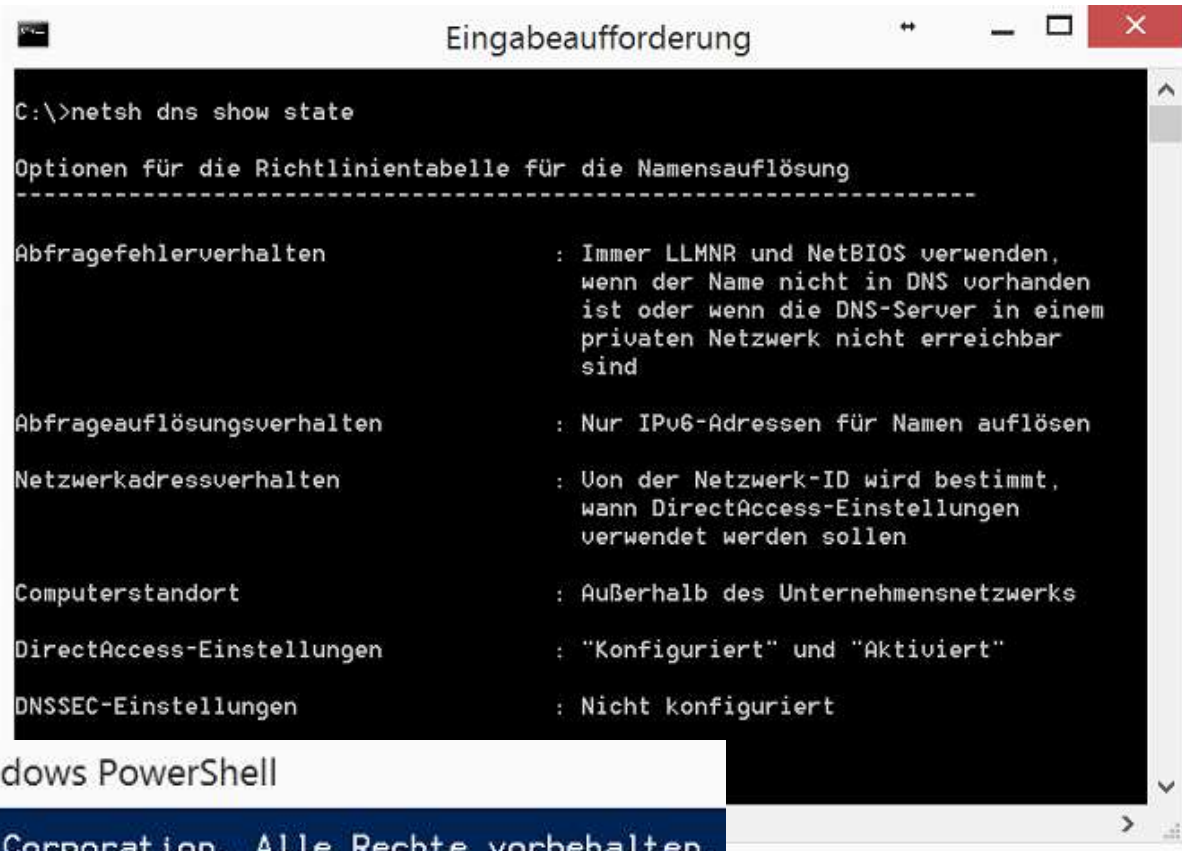
- Windows Firewall



The screenshot shows the Windows Firewall control panel window. The left sidebar is expanded to 'Verbindungssicherheitsregeln'. The main area displays a table of connection security rules.

Name	Aktivi...	Endpunkt 1	Endpunkt 2
DirectAccess Policy-ClientToCorpSimplified	Ja	Beliebig	2002:5042:1
DirectAccess Policy-ClientToDNS64NAT64Prefix...	Ja	Beliebig	fd68:30cd:7
DirectAccess Policy-ClientToNlaExempt	Ja	2002:5042:1...	2002:5042:1

- netsh dns show state



```
C:\>netsh dns show state

Optionen für die Richtlinientabelle für die Namensauflösung
-----

Abfragefehlerverhalten           : Immer LLMNR und NetBIOS verwenden,
                                   wenn der Name nicht in DNS vorhanden
                                   ist oder wenn die DNS-Server in einem
                                   privaten Netzwerk nicht erreichbar
                                   sind

Abfrageauflösungsverhalten       : Nur IPv6-Adressen für Namen auflösen

Netzwerkadressverhalten          : Von der Netzwerk-ID wird bestimmt,
                                   wann DirectAccess-Einstellungen
                                   verwendet werden sollen

Computerstandort                 : Außerhalb des Unternehmensnetzwerks

DirectAccess-Einstellungen       : "Konfiguriert" und "Aktiviert"

DNSSEC-Einstellungen             : Nicht konfiguriert
```

- get-NetIPHttpsState



```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. Alle Rechte vorbehalten.

PS C:\> get-NetIPHttpsState

LastErrorCode   : 0x0
InterfaceStatus : IPHTTPS interface active
```

Kurz vorm Ziel

Vom Client zum Service

LAN, WAN, Internet, MPLS, VPN



Direct Access ist...

- ... eine faszinierende Technologie
 - ... einfach und schnell installiert
 - ... Bestandteil von Windows
 - ... „konfigurationsfrei“ auf dem Client
 - ... konfigurationsarm auf dem Server
 - ... IPv6 sollte Sie nicht abschrecken.
-
- Einschränkungen bleiben
 - IPv4-Only Hosts sind nur über „Namen“ erreichbar
 - Clientsoftware muss IPv6 unterstützen
 - Windows Enterprise Version als Desktop

Fragen?



Kontakt:

Frank Carius, frank.carius@netatwork.de
Net at Work GmbH, Am Hoppenhof 32 A, Paderborn
+49 (5251) 304 600